Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT & TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: **Alan Boulanger**	§	Attorney Docket No.:**RSW920030105US1**
Serial No.: **10/774,017**	§	Examiner: **Trang T. Doan**
Filed: **February 5, 2004**	§	Group Art Unit: **2431**
Title: **OPERATING A COMMUNICATION NETWORK THROUGH USE OF BLOCKING MEASURES FOR RESPONDING TO COMMUNICATION TRAFFIC ANOMALIES**	§	Confirmation No.**7930**

APPEAL BRIEF UNDER 37 C.F.R. 41.37

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the Appeal of the Examiner's final rejection of Claims 1-30 in the above-identified application. A Notice of Appeal is filed concurrently herewith. No extensions of time or additional fees are believed to be required. If, however, any additional fees are required, please charge those fees to IBM Corporation Deposit Account No. **09-0457**.

REAL PARTY IN INTEREST

The real party in interest in the present Appeal is International Business Machines Corporation, the Assignee of the present application as evidenced by the assignment recorded at Frame 014971 of Reel 0014.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants, the Appellants' legal representative, or assignee, which directly affect or would be directly affected by or have a bearing on the Board's decision in the pending Appeal.

STATUS OF CLAIMS

Claims 1-30 were originally presented. Claims 1-30, which comprise all pending claims, stand finally rejected by the Examiner as noted in the Final Office Action dated October 17, 2008. The rejection of Claims 1-30 is appealed.

STATUS OF AMENDMENTS

Appellants' Amendment A, dated July 11, 2008, was entered by the Examiner. No amendments to the claims have been proposed or entered subsequent to the final rejection that leads to this appeal.

SUMMARY OF THE CLAIMED INVENTIONS

Independent Claim 1 recites a method for operating a communication network (Page 5, lines 18-34; Page 6, lines 1-6; FIG. 1). According to the method, communication traffic is autonomously monitored at a communication port for an anomalous traffic (Page 7, ¶[lines 9-15; Page 8, lines 25-30). An anomaly in detected in the communication traffic at a plurality of nodes in the communication network, wherein the anomaly is an attack other than a worm or virus (Page 8, lines 25-33; Page 9, lines 1-14; Figure 4, block 400). A first blocking measure A that stops the anomalous traffic is independently applied at respective ones of the plurality of nodes to the anomalous traffic (Page 9, lines 15-19; Figure 4, block 405). A second blocking measure B is independently determined, at the respective ones of the plurality of nodes such that application of a logical combination of the first blocking measure A and the second blocking

measure B to stop the anomalous traffic (Page 9, lines 19-25; Figure 4, block 410, Page 10, lines 21-24; Figure 5, block 505).

In addition to the features of independent Claim 1, Claim 2 recites that the independently determining step of independent Claim 1 further includes applying a logical combination of A and a second blocking measure B given by (A & !B) (Page 2, lines 21-26; FIG. 5, block 510) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B) (Page 2, lines 21-26, FIG. 5, block 505) (Page 10, lines 9-11; Page 10, lines 21-24; Figure 5, block 510). Enforcing the logical combination (A & !B), if the logical combination (A & !B) stops the anomalous traffic (Page 10, lines 21-24; Figure 5, block 510).

In addition to the features of Claims 1-2, Claim 3 recites independently determining a third blocking measure C (Page 2, lines 27-31; Page 11, lines 1-19), at the respective ones of the plurality of nodes, such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & !B) stops the anomalous traffic (Page 11, lines 8-12).

In addition to the features of Claims 1-2, Claim 4 recites that the independently determining step of independent Claim 1 further includes applying a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic (Page 9, lines 19-25; Figure 4, block 410, Page 10, lines 21-24; Figure 5, blocks 505, 520, and 535). Enforcing the logical combination (A & B), if the logical combination (A & B) stops the anomalous traffic (Page 9, lines 19-25; Figure 4, block 410, Page 10, lines 21-24; Figure 5, blocks 505 and 535).

In addition to the features of Claims 1-2 and 4, Claim 5 recites independently determining a third blocking measure C, at the respective ones of the plurality of nodes, such that application of a logical combination of (A & B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) stops the anomalous traffic (Page 11, lines 8-19).

In addition to the features of Claims 1-2 and 4, Claim 6 recites determining a third blocking measure C, at the respective ones of the plurality of nodes, such that application of a logical combination of A and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) does not stop the anomalous traffic (Page 11, lines 8-12).

In addition to the features of independent Claim 1, Claim 7 recites that the detecting step of independent Claim 1 further include comparing the communication traffic to at least one anomaly factor (Page 9, lines 1-14). Detecting the anomaly in the communication traffic at the plurality of nodes in the communication network if the at least one anomaly factor is present in the communication traffic (Page 9 lines 15-25).

In addition to the features of independent Claim 1, Claim 8 recites assigning a severity to the detected anomaly (Page 9, lines 26-29) and wherein the step of independently applying the first blocking measure A to the anomalous traffic further comprises independently applying the first blocking measure A to the anomalous traffic at each of the plurality of nodes in the communication network that stops or reduces the flow of the anomalous traffic based on the severity of the detected anomaly (Page 9, lines 30-34).

In addition to the features of independent Claim 1, Claim 9 recites intentionally inserting the anomaly in the communication traffic (Page 12, lines 21-28). Associating the first blocking measure A and the second blocking measure B with the anomaly (Page 12, lines 28-321).

Independent Claim 10 recites a method for operating a communication network (Page 5, lines 18-34; Page 6, lines 1-6; FIG. 1). According to the method, an anomaly in detected in the communication traffic at a plurality of nodes in the communication network (Page 8, lines 25-33; Page 9, lines 1-14; Figure 4, block 400). A first blocking measure A is synchronously applied at respective ones of the plurality of nodes that stops the anomalous traffic (Page 3, lines 16-30; Page 9, lines 15-19; Figure 4, block 405). A second blocking measure B is synchronously determined, at the respective ones of the plurality of nodes such that the application of a logical

combination of the first blocking measure A and the second blocking measure B stops the anomalous traffic (Page 3, lines 16-30; Page 9, lines 19-25; Figure 4, block 410, Page 10, lines 21-24; Figure 5, block 505).

Independent Claim 11 recites a system (page 4, lines 1-3 and lines 28-30) for operating a communication network (Page 5, lines 18-34; Page 6, lines 1-6; FIG. 1) including a processor (page 6, line 11; FIG. 2, processor 220) and a program means executing on the processor (page 8, lines 6-13). The program means executing on the processor further includes: means for autonomously monitoring communication traffic at a communication port for an anomalous traffic (Page 7, ¶[lines 9-15; Page 8, lines 25-30); means for detecting an anomaly in communication traffic at a plurality of nodes in the communication network, wherein the anomaly is an attack other than a worm or virus (Page 8, lines 25-33; Page 9, lines 1-14; Figure 4, block 400); means for independently applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic (Page 9, lines 15-19; Figure 4, block 405); and means for independently determining, at the respective ones of the plurality of nodes a, second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to stop the anomalous traffic (Page 9, lines 19-25; Figure 4, block 410, Page 10, lines 21-24; Figure 5, block 505).

In addition to the features of independent Claim 11, Claim 12 recites that the means for independently determining of independent Claim 11 further includes: means for applying a logical combination of A and a second blocking measure B given by (A & !B) (Page 2, lines 21-26; FIG. 5, block 510) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B) (Page 2, lines 21-26; FIG. 5, block 505) (Page 10, lines 9-11; Page 10, lines 21-24; Figure 5, block 510); and means for enforcing the logical combination (A & !B), if the logical combination (A & !B) stops the anomalous traffic (Page 10, lines 21-24; Figure 5, block 510).

In addition to the features of Claims 11-12, Claim 13 recites means for independently determining a third blocking measure C (Page 2, lines 27-31; Page 11, lines 1-19), at the

respective ones of the plurality of nodes, such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & !B) stops the anomalous traffic (Page 11, lines 8-12).

In addition to the features of Claims 11-12, Claim 14 recites that the means for independently determining of independent Claim 11 further includes: applying a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic (Page 9, lines 19-25; Figure 4, block 410, Page 10, lines 21-24; Figure 5, blocks 505, 520, and 535); and enforcing the logical combination (A & B), if the logical combination (A & B) stops the anomalous traffic (Page 9, lines 19-25; Figure 4, block 410, Page 10, lines 21-24; Figure 5, blocks 505 and 535).

In addition to the features of Claims 11-12 and 14, Claim 15 recites means for independently determining a third blocking measure C, at the respective ones of the plurality of nodes, such that application of a logical combination of (A & B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) stops the anomalous traffic (Page 11, lines 8-19).

In addition to the features of Claims 11-12 and 14, Claim 16 recites means for determining a third blocking measure C, at the respective ones of the plurality of nodes, such that application of a logical combination of A and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) does not stop the anomalous traffic (Page 11, lines 8-12).

In addition to the features of independent Claim 11, Claim 17 recites that the means for detecting an anomaly of independent Claim 11 further includes means for comparing the communication traffic to at least one anomaly factor (Page 9, lines 1-14), and means for detecting the anomaly in the communication traffic at the plurality of nodes in the communication network if the at least one anomaly factor is present in the communication traffic (Page 9 lines 15-25).

In addition to the features of independent Claim 11, Claim 18 recites means for assigning a severity to the detected anomaly (Page 9, lines 26-29), and wherein the means for independently applying the first blocking measure A to the anomalous traffic further comprises means for independently applying the first blocking measure A to the anomalous traffic at each of the plurality of nodes in the communication network that stops or reduces the flow of the anomalous traffic based on the severity of the detected anomaly (Page 9, lines 30-34).

In addition to the features of independent Claim 11, Claim 19 recites means for intentionally inserting the anomaly in the communication traffic (Page 12, lines 21-28), and means for associating the first blocking measure A and the second blocking measure B with the anomaly (Page 12, lines 28-321).

Independent Claim 20 recites a system (page 4, lines 1-3 and lines 28-30) for operating a communication network (Page 5, lines 18-34; Page 6, lines 1-6; FIG. 1). The system further includes: means for detecting an anomaly in the communication traffic at a plurality of nodes in the communication network (Page 8, lines 25-33; Page 9, lines 1-14; Figure 4, block 400); means for synchronously applying a first blocking measure A at respective ones of the plurality of nodes that stops the anomalous traffic (Page 3, lines 16-30; Page 9, lines 15-19; Figure 4, block 405); and means for synchronously determining A second blocking measure B at the respective ones of the plurality of nodes such that the application of a logical combination of the first blocking measure A and the second blocking measure B stops the anomalous traffic (Page 3, lines 16-30; Page 9, lines 19-25; Figure 4, block 410, Page 10, lines 21-24; Figure 5, block 505).

Independent Claim 21 recites a computer program product (Page 4, lines 28-30) for operating a communication network (Page 5, lines 18-34; Page 6, lines 1-6; FIG. 1) including a tangible computer storage medium (Page 4, lines 31-33; Page 5, lines 1-4; FIG. 2, storage system 225) having computer readable program code (Page 4, lines 31-33; Page 5, lines 1-4; FIG. 3, blocking measure processing 320) embodied therein. The computer readable program code further includes: computer readable program code configured to autonomously monitor communication traffic at a communication port for an anomalous traffic (Page 7, ¶[lines 9-15; Page 8, lines 25-30); computer readable program code configured to detect an anomaly in

communication traffic at a plurality of nodes in the communication network, wherein the anomaly is an attack other than a worm or virus (Page 8, lines 25-33; Page 9, lines 1-14; Figure 4, block 400); computer readable program code configured to independently apply, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic (Page 9, lines 15-19; Figure 4, block 405); and computer readable program code configured to independently determine, at the respective ones of the plurality of nodes a, second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to stop the anomalous traffic (Page 9, lines 19-25; Figure 4, block 410, Page 10, lines 21-24; Figure 5, block 505).

In addition to the features of independent Claim 21, Claim 22 recites that the computer readable program code of independent Claim 21 configured to independently determine further includes: computer readable program code configured to apply a logical combination of A and a second blocking measure B given by (A & !B) (Page 2, lines 21-26; FIG. 5, block 510) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B) (Page 2, lines 21-26; FIG. 5, block 505) (Page 10, lines 9-11; Page 10, lines 21-24; Figure 5, block 510); and computer readable program code configured to enforce the logical combination (A & !B), if the logical combination (A & !B) stops the anomalous traffic (Page 10, lines 21-24; Figure 5, block 510).

In addition to the features of Claims 21-22, Claim 23 recites computer readable program code configured to independently determine a third blocking measure C (Page 2, lines 27-31; Page 11, lines 1-19), at the respective ones of the plurality of nodes, such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & !B) stops the anomalous traffic (Page 11, lines 8-12).

In addition to the features of Claims 21-22, Claim 24 recites that the computer readable program code of independent Claim 21 that is configured to independently determine further includes: computer readable program code configured to apply a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic

(Page 9, lines 19-25; Figure 4, block 410, Page 10, lines 21-24; Figure 5, blocks 505, 520, and 535); and computer readable program code configured to enforce the logical combination (A & B), if the logical combination (A & B) stops the anomalous traffic (Page 9, lines 19-25; Figure 4, block 410, Page 10, lines 21-24; Figure 5, blocks 505 and 535).

In addition to the features of Claims 21-22 and 24, Claim 25 recites computer readable program code configured to independently determine a third blocking measure C, at the respective ones of the plurality of nodes, such that application of a logical combination of (A & B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) stops the anomalous traffic (Page 11, lines 8-19).

In addition to the features of Claims 21-22 and 24, Claim 26 recites computer readable program code configured to determine a third blocking measure C, at the respective ones of the plurality of nodes, such that application of a logical combination of A and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) does not stop the anomalous traffic (Page 11, lines 8-12).

In addition to the features of independent Claim 21, Claim 27 recites that the computer readable program code of independent Claim 11 that is configured to detect an anomaly further includes computer readable program code configured to compare the communication traffic to at least one anomaly factor (Page 9, lines 1-14), and computer readable program code configured to detect the anomaly in the communication traffic at the plurality of nodes in the communication network if the at least one anomaly factor is present in the communication traffic (Page 9 lines 15-25).

In addition to the features of independent Claim 21, Claim 28 recites computer readable program code configured to assign a severity to the detected anomaly (Page 9, lines 26-29), and wherein the computer readable program code is further configured to independently apply the first blocking measure A to the anomalous traffic further comprises means for independently applying the first blocking measure A to the anomalous traffic at each of the plurality of nodes in

the communication network that stops or reduces the flow of the anomalous traffic based on the severity of the detected anomaly (Page 9, lines 30-34).

In addition to the features of independent Claim 21, Claim 29 recites computer readable program code configured to intentionally insert the anomaly in the communication traffic (Page 12, lines 21-28), and computer readable program code configured to associate the first blocking measure A and the second blocking measure B with the anomaly (Page 12, lines 28-321).

Independent Claim 30 recites a computer program product (Page 4, lines 28-30) for operating a communication network (Page 5, lines 18-34; Page 6, lines 1-6; FIG. 1) including a tangible computer storage medium (Page 4, lines 31-33; Page 5, lines 1-4; FIG. 2, storage system 225) having computer readable program code (Page 4, lines 31-33; Page 5, lines 1-4; FIG. 3, blocking measure processing 320) embodied therein. The computer readable program code further includes: computer readable program code configured to detect an anomaly in communication traffic at a plurality of nodes in the communication network (Page 8, lines 25-33; Page 9, lines 1-14; Figure 4, block 400); computer readable program code configured to synchronously apply, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic (Page 3, lines 16-30; Page 9, lines 15-19; Figure 4, block 405); and computer readable program code configured to synchronously determine, at the respective ones of the plurality of nodes a, second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to stop the anomalous traffic (Page 3, lines 16-30; Page 9, lines 19-25; Figure 4, block 410, Page 10, lines 21-24; Figure 5, block 505).

GROUNDS OF REJECTION

The grounds of rejection to be reviewed on appeal are:

(a) the final rejection of Claims 20, 21-30 under 35 U.S.C. § 101 as being directed to non-statutory subject matter; and

(b) the final rejection of Claims 1-30 under 35 U.S.C. § 102 (b) as being anticipated by U.S. Patent No. 6,738,814 to Cox et al. (hereafter *Cox*).

ARGUMENT

I. Rejections of Claims 20-30 under 35 U.S.C. § 101

On page 3 of the Final Office Action, Claims 20 and 21-30 are rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. The § 101 rejection is not well founded and should be reversed.

A. The Rejection of Claims 21-30 under 35 U.S.C. § 101 should be reversed

The final rejection of Claims 21-30 under 35 U.S.C. § 101 should be reversed because Claims 21-30 are clearly directed to statutory subject matter.

With respect to Claims 21-30, Appellants' example Claim 21 recites a "tangible computer storage medium having computer readable program code embodied therein". At page 6, lines 11-15 of the specification, there is defined a physical storage structure (storage system 225) of a data processing system. Therefore, the recitation within the claims clearly defines a physical structure (i.e. the storage medium) which complies with a first portion of 35 U.S.C. § 101. Furthermore, Appellants' Claim 21 recites a tangible computer storage medium having computer readable program code which executes on a processor to perform the tangible result of applying a first blocking measure and determining a second blocking measure. The tangible result provided within the claim is the product of the functional steps of: (1) "autonomously monitor", (2) "detect an anomaly", (3) "independently apply", and (4) "independently determine" as recited in Appellants' Claim 21. The tangible result portion of 35 U.S.C. § 101 is also complied with. The rejection of Claims 21-30 under 35 U.S.C. § 101 as directed to non-statutory subject matter should therefore be reversed.

B. The Rejection of Claim 20 under 35 U.S.C. § 101 should be reversed

The final rejection of exemplary Claim 20 under 35 U.S.C. § 101 should be reversed.

With respect to Appellants' Claim 20, lines 20-24 of the specification recite a data processing system that provides a processor and memory that may be used for determining blocking measures for responding to communication traffic anomalies. The "means" as recited in Applicants' Claim 20 refer to the processor of the data processing system executing specific program instructions to generate the specific functions indicated by the claim elements. The rejection of Claim 20 under 35 U.S.C. § 101 as directed to non-statutory subject matter should therefore be reversed.

II. Rejections of Claims 1-30 under 35 U.S.C. § 102

On page 4 of the Final Office Action, Claims 1-30 are rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 6,738,814 to *Cox* et al. The rejection is not well founded and should be reversed.

A. The Rejection of Claim 1 under 35 U.S.C. § 102(b) based on *Cox* should be reversed

The rejection of Claim 1 as anticipated by *Cox* should be reversed because *Cox* does not disclose the following features of exemplary Claim 1:

> independently applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and
>
> independently determining, at the respective ones of the plurality of nodes, a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to stop the anomalous traffic.

With respect to the above features of Claim 1, page 4 of the Final Office Action relies upon col. 3, lines 30-54 and col. 4, lines 54-61 of *Cox*. The cited sections of *Cox*, however, do not disclose applying a first blocking measure or determining a combination of a first blocking measure and a second measure that would stop anomalous traffic.

Appellants respectfully traverse the Examiner's position because the sections of *Cox* cited by the Examiner do not disclose two (i.e. first and second) blocking measures or determining a combination of the first and second blocking measures that stops anomalous traffic, as set forth in Appellants' Claim 1. *Cox* discloses a single process that analyzes an incoming packet against known malicious patterns, and in response to detecting a malicious packet, drops the malicious packet or denies a connection request of the sender of the malicious packet. Appellants' claimed invention, in contrast, recites determining and applying a combination of the first blocking measure and a second blocking measure to stop anomalous traffic. In this manner, the invention recited in Claim 1 uses a combination of the two blocking measures to only block anomalous traffic at specific nodes, while allowing valid traffic to pass through. Without the Appellants' claimed technique of applying two blocking measures, the valid traffic may be otherwise blocked utilizing conventional techniques such as those taught by *Cox* (see, for example, page 9, lines 15-30 of the specification).

Because *Cox* does not disclose the claimed "applying" and "determining" steps related to two blocking measures as is recited in Appellants' Claim 1, the rejection of Claim 1 and its dependent claims under 35 U.S.C. § 102 as anticipated by *Cox* is not well founded and should be reversed. Additionally the claimed "applying" and "determining" steps recited in Appellants' Claim 1 are also not suggested by *Cox*.

B. The Rejection of Claim 10 under 35 U.S.C. § 102(b) based on *Cox* should be reversed

The rejection of Claim 10 as anticipated by *Cox* should be reversed because *Cox* does not disclose the following features of exemplary Claim 10:

> synchronously applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and
>
> synchronously determining, at the respective ones of the plurality of nodes, a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to stop the anomalous traffic.

With respect to the above features of Claim 10, page 4 of the Final Office Action relies upon col. 3, lines 30-54 and col. 4, lines 54-61 of *Cox*. The cited sections of *Cox*, however, do not disclose synchronously applying a first blocking measure or synchronously determining a combination of a first blocking measure and a second measure that would stop anomalous traffic.

Appellants respectfully traverse the Examiner's position because the sections of *Cox* cited by the Examiner do not disclose two (i.e. first and second) blocking measures or determining a combination of the first and second blocking measures that stops anomalous traffic, as set forth in Appellants' Claim 10. *Cox* discloses a single process that analyzes an incoming packet against known malicious patterns, and in response to detecting a malicious packet, drops the malicious packet or denies a connection request of the sender of the malicious packet. Appellants' claimed invention in contrast recites synchronously determining and synchronously applying a combination of the first blocking measure and a second blocking measure across a plurality of nodes in a communication network to stop anomalous traffic. In this manner, the invention recited in Claim 10 uses a combination of the two blocking measures to only block anomalous traffic synchronously across a plurality of nodes, while allowing valid traffic to pass through. Without the Appellants claimed technique of applying two blocking measures, the valid traffic may be otherwise blocked utilizing conventional techniques such as those taught by *Cox* (see, for example, page 9, lines 15-30 of the specification).

Because *Cox* does not disclose the claimed "synchronously applying" and "synchronously determining" steps related to two blocking measures as is recited in Appellants' Claim 10, the rejection of Claim 10 under 35 U.S.C. § 102 as anticipated by *Cox* is not well founded and should be reversed. Additionally the claimed "synchronously applying" and "synchronously determining" steps recited in Appellants' Claim 10 are also not suggested by *Cox*.

C. The Rejection of Claim 11 under 35 U.S.C. § 102(b) based on *Cox* should be reversed

The rejection of Claim 11 as anticipated by *Cox* should be reversed because *Cox* does not disclose the following features of exemplary Claim 11:

> means for independently applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and
>
> means for independently determining, at the respective ones of the plurality of nodes a, second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to stop the anomalous traffic.

With respect to the above features of Claim 11, page 4 of the Final Office Action relies upon col. 3, lines 30-54 and col. 4, lines 54-61 of *Cox*. The cited sections of *Cox*, however, do not disclose applying a first blocking measure or determining a combination of a first blocking measure and a second measure that would stop anomalous traffic.

Appellants respectfully traverse the Examiner's position because the sections of *Cox* cited by the Examiner do not disclose two (i.e. first and second) blocking measures or determining a combination of the first and second blocking measures that stops anomalous traffic, as set forth in Appellants' Claim 11. *Cox* discloses a single process that analyzes an incoming packet against known malicious patterns, and in response to detecting a malicious packet, drops the malicious packet or denies a connection request of the sender of the malicious packet. Appellants' claimed invention in contrast recites determining and applying a combination of the first blocking measure and a second blocking measure to stop anomalous traffic. In this manner, the invention recited in Claim 11 uses a combination of the two blocking measures to only block anomalous traffic at specific nodes, while allowing valid traffic to pass through. Without the Appellants claimed technique of applying two blocking measures, the valid traffic may be otherwise blocked utilizing conventional techniques such as those taught by *Cox* (see, for example, page 9, lines 15-30 of the specification).

Because *Cox* does not disclose the claimed "applying" and "determining" steps related to two blocking measures as is recited in Appellants' Claim 11, the rejection of Claim 11 and its dependent claims under 35 U.S.C. § 102 as anticipated by *Cox* is not well founded and should be reversed. Additionally the claimed "applying" and "determining" steps recited in Appellants' Claim 11 are also not suggested by *Cox*.

D. The Rejection of Claim 20 under 35 U.S.C. § 102(b) based on *Cox* should be reversed

The rejection of Claim 20 as anticipated by *Cox* should be reversed because *Cox* does not disclose the following features of exemplary Claim 20:

> means for synchronously applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and
>
> means for synchronously determining a second blocking measure B at the respective ones of the plurality of nodes such that application of a logical combination of the first blocking measure A and the second blocking measure B to stop the anomalous traffic.

With respect to the above features of Claim 20, page 4 of the Final Office Action relies upon col. 3, lines 30-54 and col. 4, lines 54-61 of *Cox*. The cited sections of *Cox*, however, do not disclose synchronously applying a first blocking measure or synchronously determining a combination of a first blocking measure and a second measure that would stop anomalous traffic.

Appellants respectfully traverse the Examiner's position because the sections of *Cox* cited by the Examiner do not disclose two (i.e. first and second) blocking measures or determining a combination of the first and second blocking measures that stops anomalous traffic, as set forth in Appellants' Claim 20. *Cox* discloses a single process that analyzes an incoming packet against known malicious patterns, and in response to detecting a malicious packet, drops the malicious packet or denies a connection request of the sender of the malicious packet. Appellants' claimed invention in contrast recites synchronously determining and

synchronously applying a combination of the first blocking measure and a second blocking measure across a plurality of nodes in a communication network to stop anomalous traffic. In this manner, the invention recited in Claim 20 uses a combination of the two blocking measures to only block anomalous traffic synchronously across a plurality of nodes, while allowing valid traffic to pass through. Without the Appellants claimed technique of applying two blocking measures, the valid traffic may be otherwise blocked utilizing conventional techniques such as those taught by *Cox* (see, for example, page 9, lines 15-30 of the specification).

Because *Cox* does not disclose the claimed "synchronously applying" and "synchronously determining" steps related to two blocking measures as is recited in Appellants' Claim 20, the rejection of Claim 20 under 35 U.S.C. § 102 as anticipated by *Cox* is not well founded and should be reversed. Additionally the claimed "synchronously applying" and "synchronously determining" steps recited in Appellants' Claim 20 are also not suggested by *Cox*.

E. The Rejection of Claim 21 under 35 U.S.C. § 102(b) based on *Cox* should be reversed

The rejection of Claim 21 as anticipated by *Cox* should be reversed because *Cox* does not disclose the following features of exemplary Claim 21:

> computer readable program code configured to independently apply, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and
>
> computer readable program code configured to independently determine at the respective ones of the plurality of nodes a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to stop the anomalous traffic.

With respect to the above features of Claim 21, page 4 of the Final Office Action relies upon col. 3, lines 30-54 and col. 4, lines 54-61 of *Cox*. The cited sections of *Cox*, however, do

not disclose applying a first blocking measure or determining a combination of a first blocking measure and a second measure that would stop anomalous traffic.

Appellants respectfully traverse the Examiner's position because the sections of *Cox* cited by the Examiner do not disclose two (i.e. first and second) blocking measures or determining a combination of the first and second blocking measures that stops anomalous traffic, as set forth in Appellants' Claim 21. *Cox* discloses a single process that analyzes an incoming packet against known malicious patterns, and in response to detecting a malicious packet, drops the malicious packet or denies a connection request of the sender of the malicious packet. Appellants' claimed invention in contrast recites determining and applying a combination of the first blocking measure and a second blocking measure to stop anomalous traffic. In this manner, the invention recited in Claim 21 uses a combination of the two blocking measures to only block anomalous traffic at specific nodes, while allowing valid traffic to pass through. Without the Appellants claimed technique of applying two blocking measures, the valid traffic may be otherwise blocked utilizing conventional techniques such as those taught by *Cox* (see, for example, page 9, lines 15-30 of the specification).

Because *Cox* does not disclose the claimed "applying" and "determining" steps related to two blocking measures as is recited in Appellants' Claim 21, the rejection of Claim 21 and its dependent claims under 35 U.S.C. § 102 as anticipated by *Cox* is not well founded and should be reversed. Additionally the claimed "applying" and "determining" steps recited in Appellants' Claim 21 are also not suggested by *Cox*.

F. The Rejection of Claim 30 under 35 U.S.C. § 102(b) based on *Cox* should be reversed

The rejection of Claim 30 as anticipated by *Cox* should be reversed because *Cox* does not disclose the following features of exemplary Claim 30:

> computer readable program code configured to synchronously apply, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

computer readable program code configured to synchronously determine at the respective ones of the plurality of nodes a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to stop the anomalous traffic.

With respect to the above features of Claim 30, page 4 of the Final Office Action relies upon col. 3, lines 30-54 and col. 4, lines 54-61 of *Cox*. The cited sections of *Cox*, however, do not disclose synchronously applying a first blocking measure or synchronously determining a combination of a first blocking measure and a second measure that would stop anomalous traffic.

Appellants respectfully traverse the Examiner's position because the sections of *Cox* cited by the Examiner do not disclose two (i.e. first and second) blocking measures or determining a combination of the first and second blocking measures that stops anomalous traffic, as set forth in Appellants' Claim 30. *Cox* discloses a single process that analyzes an incoming packet against known malicious patterns, and in response to detecting a malicious packet, drops the malicious packet or denies a connection request of the sender of the malicious packet. Appellants' claimed invention in contrast recites synchronously determining and synchronously applying a combination of the first blocking measure and a second blocking measure across a plurality of nodes in a communication network to stop anomalous traffic. In this manner, the invention recited in Claim 30 uses a combination of the two blocking measures to only block anomalous traffic synchronously across a plurality of nodes, while allowing valid traffic to pass through. Without the Appellants claimed technique of applying two blocking measures, the valid traffic may be otherwise blocked utilizing conventional techniques such as those taught by *Cox* (see, for example, page 9, lines 15-30 of the specification).

Because *Cox* does not disclose the claimed "synchronously applying" and "synchronously determining" steps related to two blocking measures as is recited in Appellants' Claim 30, the rejection of Claim 30 under 35 U.S.C. § 102 as anticipated by *Cox* is not well founded and should be reversed. Additionally the claimed "synchronously applying" and "synchronously determining" steps recited in Appellants' Claim 30 are also not suggested by *Cox*.

G. The Rejection of Claim 2, 12, and 22 under 35 U.S.C. § 102(b) based on *Cox* should be reversed

In addition to the reasons set forth with reference to Claim 1 (and similar Claims 11 and 21) above, the final rejection of Claims 2, 12, and 22 should also be reversed because *Cox* does not disclose "applying a logical combination of A and a second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B)," as recited in Appellants' Claims 2, 12, and 22.

With reference to Claim 2, at page 3 of the Final Office Action the Examiner cites column 4 lines 28-61 of *Cox*. The cited passage of *Cox* teaches a method for blocking spoofing or denial of service attacks (DoS) by comparing a requested connection to existing connections and in response to determining the requested connection matches an existing connection, denying the requested connection. Thus, this section of *Cox* and *Cox* as a whole does not disclose applying a logical combination (A & !B) of a first blocking measure (A) and a second blocking measures (B) that is less restrictive than a complete logical combination of the two blocking measures (A & B). *Cox* only discloses denying a connection request in response to determining that a computer having the same address is already connected to a network. Appellants' Claim 2 in contrast recites applying a logical combination of two blocking measures that may be applied to a traffic stream to block or reduce a flow of traffic anomalies, while still allowing valid traffic to pass through (see, for example, page 12, lines 21-32; and page 13, lines 1-4 of the specification). Because *Cox* does not disclose applying a logical combination of blocking measures as recited in Claim 2, the rejection of Claims 2, 12, and 22 under 35 U.S.C. § 102 should be reversed. Additionally the claimed applying a logical combination of blocking measures as recited in Appellants' Claim 2 are also not suggested by *Cox*.

H. Rejection of Claim 3, 13, and 23 under 35 U.S.C. § 102(b) based on *Cox* should be reversed

The final rejection of Claims 3, 13, and 23 under 35 U.S.C. § 102 as anticipated by *Cox* should be reversed for the reasons set forth above with reference to underlying Claims 1-2, 11-12, and 21-22, respectively.

I. Rejection of Claim 4, 14, and 24 under 35 U.S.C. § 102(b) based on *Cox* should be reversed

The final rejection of Claims 4, 14, and 24 under 35 U.S.C. § 102 as anticipated by *Cox* should be reversed for the reasons set forth above with reference to underlying Claims 1-2, 11-12, and 21-22, respectively.

J. Rejection of Claim 5, 15, and 25 under 35 U.S.C. § 102(b) based on *Cox* should be reversed

The final rejection of Claims 5, 14, and 25 under 35 U.S.C. § 102 as anticipated by *Cox* should be reversed for the reasons set forth above with reference to underlying Claims 1-2 and 4, 11-12 and 14, and 21-22 and 24, respectively.

K. Rejection of Claim 6, 16, and 26 under 35 U.S.C. § 102(b) based on *Cox* should be reversed

The final rejection of Claims 6, 16, and 26 under 35 U.S.C. § 102 as anticipated by *Cox* should be reversed for the reasons set forth above with reference to underlying Claims 1-2 and 4, 11-12 and 14, and 21-22 and 24, respectively.

L. Rejection of Claim 7, 17, and 27 under 35 U.S.C. § 102(b) based on *Cox* should be reversed

The final rejection of Claims 7, 17, and 27 under 35 U.S.C. § 102 as anticipated by *Cox* should be reversed for the reasons set forth above with reference to underlying Claims 1, 11, and 21, respectively.

M. Rejection of Claim 8, 18, and 28 under 35 U.S.C. § 102(b) based on *Cox* should be reversed

The final rejection of Claims 8, 18, and 28 under 35 U.S.C. § 102 as anticipated by *Cox* should be reversed for the reasons set forth above with reference to underlying Claims 1, 11, and 21, respectively.

N. Rejection of Claim 9, 19, and 29 under 35 U.S.C. § 102(b) based on *Cox* should be reversed

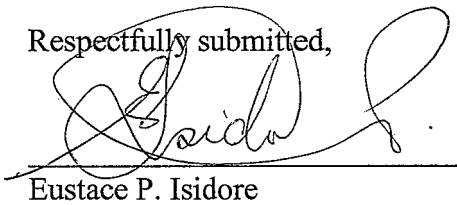
The final rejection of Claims 9, 19, and 29 under 35 U.S.C. § 102 as anticipated by *Cox* should be reversed for the reasons set forth above with reference to underlying Claims 1, 11, and 21, respectively.

CONCLUSION

The foregoing remarks demonstrate that *Cox* does not disclose each and every feature of Appellants' Claims 1-30 as required to support a rejection under 35 U.S.C. § 102(b). Appellants have also shown that the Claims recite statutory subject matter under 35 U.S.C. § 101. Appellants therefore respectfully request the Board reverse the rejection of each of Claims 1-30.

Applicants further respectfully request the Examiner contact the undersigned attorney of record at 512.343.6116 if such would further or expedite the prosecution of the present Application.

Respectfully submitted,



Eustace P. Isidore
Reg. No. 56,104
DILLON & YUDELL LLP
8911 N. Capital of Texas Highway
Suite 2110
Austin, Texas 78759
(512) 343-6116
ATTORNEY FOR APPELLANTS

CLAIMS APPENDIX

1. A method of operating a communication network, comprising:

autonomously monitoring communication traffic at a communication port for an anomalous traffic;

detecting an anomaly in communication traffic at a plurality of nodes in the communication network, wherein the anomaly is an attack other than a worm or virus;

independently applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

independently determining, at the respective ones of the plurality of nodes, a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to stop the anomalous traffic.

2. The method of claim 1, wherein independently determining the second blocking measure B comprises:

applying a logical combination of A and a second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and

enforcing the logical combination (A & !B), if the logical combination (A & !B) stops the anomalous traffic.

3. The method of claim 2, further comprising:

independently determining a third blocking measure C, at the respective ones of the plurality of nodes, such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & !B) stops the anomalous traffic.

4. The method of claim 2, wherein independently determining the second blocking measure B further comprises:

applying a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and

enforcing the logical combination (A & B), if the logical combination (A & B) stops the anomalous traffic.

5. The method of claim 4, further comprising:

independently determining a third blocking measure C, at the respective ones of the plurality of nodes, such that application of a logical combination of (A & B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) stops the anomalous traffic.

6. The method of claim 4, further comprising:

determining a third blocking measure C, at the respective ones of the plurality of nodes, such that application of a logical combination of A and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) does not stop the anomalous traffic.

7. The method of claim 1, wherein detecting an anomaly in the communication traffic comprises:

comparing the communication traffic to at least one anomaly factor; and

detecting the anomaly in the communication traffic at the plurality of nodes in the communication network if the at least one anomaly factor is present in the communication traffic.

8. The method of claim 1, further comprising:

assigning a severity to the detected anomaly; and

wherein independently applying the first blocking measure A to the anomalous traffic comprises independently applying the first blocking measure A to the anomalous traffic at each of the plurality of nodes in the communication network that stops or reduces the flow of the anomalous traffic based on the severity of the detected anomaly.

9. The method of claim 1, further comprising:

intentionally inserting the anomaly in the communication traffic; and

associating the first blocking measure A and the second blocking measure B with the anomaly.

10. A method of operating a communication network, comprising:

detecting an anomaly in communication traffic at a plurality of nodes in the communication network;

synchronously applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

synchronously determining, at the respective ones of the plurality of nodes, a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to stop the anomalous traffic.

11. A system for operating a communication network, comprising:

a processor;

program means executing on the processor including:

means for autonomously monitoring communication traffic at a communication port for an anomalous traffic;

means for detecting an anomaly in communication traffic at a plurality of nodes in the communication network, wherein the anomaly is an attack other than a worm or virus;

means for independently applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

means for independently determining, at the respective ones of the plurality of nodes a, second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to stop the anomalous traffic.

12. The system of claim 11, wherein the means for independently determining the second blocking measure B comprises:

means for applying a logical combination of A and a second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and

means for enforcing the logical combination (A & !B), if the logical combination (A & !B) stops the anomalous traffic.

13. The system of claim 12, further comprising:

means for independently determining, at the respective ones of the plurality of nodes, a third blocking measure C such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & !B) stops the anomalous traffic.

14. The system of claim 12, wherein the means for independently determining the second blocking measure B further comprises:

means for applying a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and

means for enforcing the logical combination (A & B), if the logical combination (A & B) stops the anomalous traffic.

15. The system of claim 14, further comprising:

means for independently determining, at the respective ones of the plurality of nodes, a third blocking measure C such that application of a logical combination of (A & B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) stops the anomalous traffic.

16. The system of claim 14, further comprising:

means for determining, at the respective ones of the plurality of nodes, a third blocking measure C such that application of a logical combination of A and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) does not stop the anomalous traffic.

17. The system of claim 11, wherein the means for detecting an anomaly in the communication traffic comprises:

means for comparing the communication traffic to at least one anomaly factor; and

means for detecting the anomaly in the communication traffic at the plurality of nodes in the communication network, if the at least one anomaly factor is present in the communication traffic.

18. The system of claim 11, further comprising:

means for assigning a severity to the detected anomaly; and

wherein the means for independently applying the first blocking measure A to the anomalous traffic comprises means for independently applying the first blocking measure A to the anomalous traffic at each of the plurality of nodes in the communication network that stops or reduces the flow of the anomalous traffic based on the severity of the detected anomaly.

19. The system of claim 11, further comprising:

means for intentionally inserting the anomaly in the communication traffic; and

means for associating the first blocking measure A and the second blocking measure B with the anomaly.

20. A system for operating a communication network, comprising:

means for detecting an anomaly in communication traffic at a plurality of nodes in the communication network;

means for synchronously applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

means for synchronously determining a second blocking measure B at the respective ones of the plurality of nodes such that application of a logical combination of the first blocking measure A and the second blocking measure B to stop the anomalous traffic.

21. A computer program product for operating a communication network, comprising:

a tangible computer storage medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code configured to autonomously monitor communication traffic at a communication port for an anomalous traffic;

computer readable program code configured to detect an anomaly in communication traffic at a plurality of nodes in the communication network, wherein the anomaly is an attack other than a worm or virus;

computer readable program code configured to independently apply, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

computer readable program code configured to independently determine at the respective ones of the plurality of nodes a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to stop the anomalous traffic.

22. The computer program product of claim 21, wherein the computer readable program code configured to independently determine the second blocking measure B comprises:

computer readable program code configured to apply a logical combination of A and a second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and

computer readable program code configured to enforce the logical combination (A & !B) if the logical combination (A & !B) stops the anomalous traffic.

23. The computer program product of claim 22, further comprising:

computer readable program code configured to independently determine, at the respective ones of the plurality of nodes, a third blocking measure C such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & !B) stops the anomalous traffic.

24. The computer program product of claim 22, wherein the computer readable program code configured to independently determine the second blocking measure B further comprises:

computer readable program code configured to apply a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and

computer readable program code configured to enforce the logical combination (A & B), if the logical combination (A & B) stops the anomalous traffic.

25. The computer program product of claim 24, further comprising:

computer readable program code configured to independently determine, at the respective ones of the plurality of nodes, a third blocking measure C such that application of a logical combination of (A & B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) stops the anomalous traffic.

26. The computer program product of claim 24, further comprising:

computer readable program code configured to determine, at the respective ones of the plurality of nodes, a third blocking measure C such that application of a logical combination of A and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & B) does not stop the anomalous traffic.

27. The computer program product of claim 21, wherein the computer readable program code configured to detect an anomaly in the communication traffic comprises:

computer readable program code configured to compare the communication traffic to at least one anomaly factor; and

computer readable program code configured to detect the anomaly in the communication traffic at the plurality of nodes in the communication network, if the at least one anomaly factor is present in the communication traffic.

28. The computer program product of claim 21, further comprising:

computer readable program code configured to assign a severity to the detected anomaly; and

wherein the computer readable program code configured to independently apply the first blocking measure A to the anomalous traffic comprises computer readable program code configured to independently apply the first blocking measure A to the anomalous traffic at each of the plurality of nodes in the communication network that stops or reduces the flow of the

anomalous traffic based on the severity of the detected anomaly.

29. The computer program product of claim 21, further comprising:

computer readable program code configured to intentionally insert the anomaly in the communication traffic; and

computer readable program code configured to associate the first blocking measure A and the second blocking measure B with the anomaly.

30. A computer program product for operating a communication network, comprising:

a tangible computer storage medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code configured to detect an anomaly in communication traffic at a plurality of nodes in the communication network;

computer readable program code configured to synchronously apply, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

computer readable program code configured to synchronously determine at the respective ones of the plurality of nodes a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to stop the anomalous traffic.

EVIDENCE APPENDIX

(NONE)

APPENDIX C
RELATED PROCEEDINGS AND INTERFERENCES

(NONE)